

Internal Control Comparisons Using COSO

By: Rachel McIntosh, Kate Arnott, and Tore Profaci

Purpose

- To test and compare internal controls of three different types of small businesses.
- See what measures are being taken, if any, to secure access to accounting information.
- Determine if organizational differences in the 3 companies may have affected the implementation of IT controls.
- After analysis, make recommendations for what controls the companies could improve.

Background

- All three companies are small and not required under SOX to be audited.
- Companies A, B, and C
- COSO will be used
- Forms provided by a CPA firm

Company A

- Environmental engineering firm
- Engaged in the business of providing ecological impact assessments, studies for construction projects and engineering consulting services for environmental, health and safety under fixed-price contracts, time-and-materials contracts and cost-plus contracts.
- 70% minority owned
- Certification under US Small Business Administration's Business Development Program, which requires yearly audits based on amount of revenue earned.
- Received unqualified opinion on financial statements for years 2010 and 2011.
- Also undergoes yearly audits from the Defense Contract Audit Agency (DCAA) to make sure in compliance with FAR regulations.

Company B

- Best described as a retail company.
- Contracts with theme parks across U.S. in order to rent space and sell specialized merchandise. Approximately 25 locations.
- Corporate office in Orlando, FL
- Run by founders children, who are now part of top management.
- Advanced computer equipment and vast graphics department.
- Required to be in compliance with IT requirements of various landlords.
- Deal with credit card transactions, so must follow PCI-DSS standards.

Company C

- Small, family owned company that specializes in aftermarket air suspension products.
- Privately owned. Owner is both CEO and president.
- Most top management positions held my by family members.
- Experiencing steady growth.
- In the past, unable to accommodate proper staffing due to limited space.
- Top management was involved in every aspect and no clear separation of duties.
- Expanded last year and created new HR department and is working on developing IT department.
- Majority of orders are made over phone or online.
- Credit card transactions prevalent, must be compliant with PCI-DSS.

COSO Background

- Established in 1985 to provide thought leadership for 3 subjects.
- In 1992 published Internal Control Integrated Framework
- Guideline for what internal controls should be.
- 5 different elements are analyzed in evaluation of internal controls

COSO Elements

Five Elements of COSO analyzed for the 3 companies:

- Control Environment- Environment the company creates for different business processes and controls.
- Risk Assessment- How effective is entity in recognizing risks and mitigating those risks.
- Control Activities- The specific controls that an entity has in place. Auditors must document specific control activities and their objectives.
- Information and Communication- There should be adequate controls to ensure prompt and accurate notification of the occurrence of a material misstatement.
- Monitoring- Involves oversight of internal controls by management or an outside party to ensure quality over a long period of time.

Table 1: Control Testing Questionnaire

Our group used 5 separate questionnaire forms based on COSO to get information regarding the controls of each company tested.

CON-CX-5.1: Entity-level Control
Form for Control Environment
35 Questions In Total

CON-CX-5.2: Entity-level Control
Form for Risk Assessment
18 Questions In Total

CON-CX-5.3: Entity-level Control Form
for Information and Communication
11 Questions In Total

CON-CX-5.4: Entity-level Control Form
for Monitoring
6 Questions In Total

CON-CX-5.5: Entity-level Control
Form for General Computer Controls
28 Questions In Total

Table 1: Control Testing Questionnaire

CON-CX-5.1: Entity-level Control Form for Control Environment

Question:

The makeup and general construction of the board of directors and its committees are appropriate and adequate given the nature of the entity.

Response:

All three had the control in place & it was effectively designed. Example comment BOD made up of 5 owners, meets monthly

Question:

Those charged with governance are sufficiently involved with the entity to address important oversight responsibilities.

Response:

All three had the control in place & it was effectively designed. Example comment all work at least 40 hours a week in office and on job sites

Question: Relationships with professional third parties are periodically reviewed to ensure the entity maintains association with reputable parties.

Response:

All three had the control in place & it was effectively designed. Example comment; D&B check, credit checks, background checks

Table 1: Control Testing Questionnaire

CON-CX-5.2: Entity-level Control Form for Risk Assessment

Question:

Entity objectives are established, communicated, and monitored. The key elements of the entity's strategic plan are communicated throughout the entity.

Response:

All three had the control in place, only 1 thought it was effectively designed. Example comment admin manual, SOP's, e-mails and verbal

Question:

The entity's assessment of fraud risk considers incentives and pressures, attitudes, and rationalizations as well as the opportunity to commit fraud.

Response:

None of the companies had a control in place, thus it wasn't effectively designed

Question:

Budgets/forecasts are updated during the year to reflect changes in the entity's activities.

Response:

Two out of three had the control in place, both thought it was effectively designed. Example comment continual and required in order to keep up with competition

Table 1: Control Testing Questionnaire

CON-CX-5.3: Entity-level Control Form for Information and Communication

Question:

Financial personnel meet with line management to discuss operating results.

Response:

All three had the control in place & it was effectively designed. Example comment monthly meetings, plus on the spot training, when errors found

Question:

Employees receive adequate information to complete their job responsibilities.

Response:

All three had the control in place & it was effectively designed. Example comment meetings and policies

Question:

Upstream communication is encouraged by management to improve performance and enhance internal control.

Response:

All three had the control in place & it was effectively designed. Example comment open door policy.

Table 1: Control Testing Questionnaire

CON-CX-5.4: Entity-level Control Form for Monitoring

Question:

Management's ongoing monitoring provides feedback on the effective design and operation of controls integrated into processes, and on the processes themselves.

Response:

All three had the control in place & it was effectively designed. Example comment yearly review and update SOPs

Question:

Reports from external sources (e.g., external auditors, regulators) are considered for their internal control implications, and timely corrective actions are identified and taken.

Response:

All three had the control in place & it was effectively designed. Example comment after reports are received managements meets to discuss.

Question:

Findings of an internal control deficiency are reported to (1) the appropriate person who is in the position to take corrective actions and, if applicable, (2) at least one level of management above that person.

Response:

All three had the control in place & it was effectively designed. Example comment communicated to the manager, as well as the Partner in charge

Table 1: Control Testing Questionnaire

CON-CX-5.5: Entity-level Control Form for General Computer Controls

Question:

IT is evaluated regularly for risks and any identified risks are appropriately addressed.

Response:

All three had the control in place , only 1 thought it it was effectively designed. Example comment in planning phase.
Outside Security risks are evaluated by a third party.SOPs

Question:

A backup and data retention policy/schedule exists, specifying how often backups are to be performed, how long they are to be retained, and where the backup media is to be stored.

Response:

All three had the control in place & it was effectively designed. Example comment back-ups are done twice a day, and backed-up to 3 separate locations.

Question:

Application data and file server recovery procedures are tested at least annually to ensure data integrity and recovery.

Response:

All three had the control in place & it was effectively designed. Example comment back-ups are tested to make sure they are occurring and data is being backed-up in its entirety

Summary - Part 1

Control Environment

- Strong and effectively designed
- Committed to accurate financial reporting
- Strong internal controls
- Recommendation: maintain regular monitoring of controls

Summary - Part 2

Risk Assessment

- Weakest and least effectively designed
- Limited to following GAAP rules
- Risk assessment and monitoring is not performed
- Recommendation: establish formal processes for fraud detection

Summary - Part 3

Information & Communication

- Strong and effectively designed
- Financial procedures clearly stated
- Open communication with top management
- Recommendation: stronger controls for tracking communication

Summary - Part 4

Monitoring

- The strongest and most effectively designed
- Good management structure
- Deficiencies reported in a timely manner
- Recommendation: continue regular monitoring

Summary - Part 5

General Computer Controls

- 2 out of 3 have effectively designed computer controls
- Strong controls over physical access and network security
- Recommendations:
 - establish and maintain formal information security policy
 - separate IT department
 - monitor credentials of outside service providers

Conclusion

Even though all three small businesses are not yet required to comply with governmental regulations, they are committed to establishing and maintaining strong internal controls.